Notice of Allowability	Application No.	Applicant(s)	
	09/970,912	ROBERTSON ET AL.	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *08/27/2007*.

2. ☒ The allowed claim(s) is/are *1,5,12,16, 22, 24, 25 and 27*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☒ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *9/7/07* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

9/13/07

DETAILED ACTION

1. Examiner initiated interview has been made to discuss the new matter rejection mailed on 04/27/2007, the applicant pointed out the support on page 6 paragraph 23-24 of applicant's disclosure, discuss 112 rejections made regarding "such as" being included in the claims, and 101 rejection made on the above same date but unamended in the applicant's response. Moreover, the allowable subject matter mailed, to move dependent claims, was not amended, in the response, but all the problems above and more has been resolved by the interview made on 9/11/07 with Madelynne Farber (45410).

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Madelynne Farber (45410).

3. Claims 1, 5, 12, 16, 22, 24, 25, and 27 are amended and claims 4, 15, 23, and 26 are canceled as follows:

1 (Currently Amended) A method of enhancing throughput of a multi-stage pipelined encryption/decryption engine for an encryption/decryption process when used with an

encryption/decryption mode of operation requiring feedback around the pipelined engine, the method comprising [the] steps of:

aggregating together multiple security contexts and establishing an entry in a bank of initial variables for each context, there being at least as many encryption/decryption security context identifiers as a predetermined number of stages in the encryption/decryption process;

receiving, for input to the multi-stage pipelined encryption/decryption engine, a source datablock for a given encryption/decryption security context identifier;

indexing according to the encryption/decryption security context identifier into the bank of initial variables to retrieve an initial variable for the source datablock, the bank comprising a plurality of initial variables for each encryption/decryption security context identifier;

generating an output datablock from the source datablock and its corresponding initial variable; [and]

replacing the initial variable in the bank of initial variables with a new seed, as determined by a selected mode of operation, for the security context identifier [.] ; and

wherein the mode of operation of the encryption/decryption process requires feedback around the encryption/decryption engine; and wherein the pipelined encryption/decryption engine is Cipher Block Chaining Mode with exception of handling of initial variables.

4. (Canceled).

5. (Currently Amended) The method of claim 1 wherein the encryption/decryption process comprises a block cipher capable of being pipelined ~~such as~~ and the

encryption/decryption process is Digital Encryption Standard (DES).

12. (Currently Amended) A multi-stage pipelined encryption engine for an encryption/decryption process when used with an encryption/decryption mode of operation requiring feedback around the stages, the encryption/decryption engine comprising:

means for aggregating together multiple security contexts and establishing an entry in a bank of initial variables for each context, there being at least as many encryption/decryption security context identifiers as a predetermined number of stages in the encryption/decryption process;

means for receiving, for input to the multi-stage pipelined encryption/decryption engine, a source datablock for a given encryption/decryption security context identifier, there being at least as many encryption/decryption security context identifiers as the predetermined number of stages in the encryption/decryption process;

means for indexing according to the encryption/decryption security context identifier into a bank of initial variables to retrieve an initial variable for the source datablock, the bank comprising a plurality of initial variables for each encryption/decryption security context identifier;

means for generating an output datablock from the source datablock and its corresponding initial variable; [and]

means for replacing the initial variable in the bank of initial variables with a new seed, as determined by a selected mode of operation, for the security context identifier [.]; and

wherein the mode of operation of the encryption/decryption process requires feedback around the encryption/decryption engine; and wherein the pipelined encryption/decryption engine is Cipher Block Chaining Mode with exception of handling of initial variables.

15. (Canceled).

16. (Currently Amended) The encryption/decryption engine of claim 12 wherein the encryption/decryption process comprises a block cipher capable of being pipelined ~~such as~~ and the encryption/decryption process is Digital Encryption Standard (DES).

22. (Currently Amended) A method of enhancing throughput of a multi-stage pipelined encryption/decryption engine for an encryption/decryption process when used with an encryption/decryption mode of operation requiring feedback around the pipelined engine, the method comprising [the] steps of:

separating one data stream into multiple interleaved data streams, each having its own encryption/decryption security context;

aggregating together the multiple security contexts and establishing an entry in a bank of initial variables for each context, there being at least as many encryption/decryption security context identifiers as a predetermined number of stages in the encryption/decryption process;

receiving, for input to the multi-stage pipelined encryption/decryption engine, a source datablock for a given encryption/decryption security context identifier ~~[, there being at least as~~

~~many encryption/decryption security context identifiers as the predetermined number of stages in the encryption/decryption process];~~

indexing according to the encryption/decryption security context identifier into the bank of initial variables to retrieve an initial variable for the source datablock, the bank comprising a plurality of initial variables for each encryption/decryption security context identifier;

generating an output datablock from the source datablock and its corresponding initial variable; [and]

replacing the initial variable in the bank of initial variables with a new seed, as determined by a selected mode of operation, for the security context identifier [.]; and

wherein the mode of operation of the encryption/decryption process requires feedback around the encryption/decryption engine; and wherein the pipelined encryption/decryption engine is Cipher Block Chaining Mode with exception of handling of initial variables.

23 (Canceled).

24. (Currently Amended) The method of claim [23] 22 wherein the encryption/decryption process comprises a block cipher capable of being pipelined ~~such as~~ and the encryption/decryption process is Digital Encryption Standard (DES).

25. (Currently Amended) A multi-stage pipelined encryption engine for an encryption/decryption process when used with an encryption/decryption mode of operation requiring feedback around the stages, the encryption/decryption engine comprising:

means for separating one data stream into multiple interleaved data streams, each having its own encryption/decryption security context ;

means for aggregating together the multiple security contexts and establishing an entry in a bank of initial variables for each context, there being at least as many encryption/decryption security context identifiers as a predetermined number of stages in the encryption/decryption process;

means for receiving, for input to the multi-stage pipelined encryption/decryption engine, a source datablock for a given encryption/decryption security context identifier, there being at least as many encryption/decryption security context identifiers as the predetermined number of stages in the encryption/decryption process;

means for indexing according to the encryption/decryption security context identifier into a bank of initial variables to retrieve an initial variable for the source datablock, the bank comprising a plurality of initial variables for each encryption/decryption security context identifier;

means for generating an output datablock from the source datablock and its corresponding initial variable; [and]

means for replacing the initial variable in the bank of initial variables with a new seed, as determined by a selected mode of operation, for the security context identifier [.]; and

wherein the mode of operation of the encryption/decryption process requires feedback around the encryption/decryption engine; and wherein the pipelined encryption/decryption engine is Cipher Block Chaining Mode with exception of handling of initial variables.

26. (Canceled).

27. (Currently Amended) The encryption/decryption engine of claim 25 wherein the encryption/decryption process comprises a block cipher capable of being pipelined ~~such as~~ and the encryption/decryption process is Digital Encryption Standard (DES).

Allowable Subject Matter

4. Claims 1, 5, 12, 16, 22, 24, 25, and 27 are allowed.

The following is an examiner's statement of reasons for allowance: The prior art fails to teach a multi-stage pipelined encryption engine comprising encryption/decryption security context in each separated data streams, establishing an entry in a bank of initial variables for each context, receiving a source datablock for a given encryption/decryption security identifier, indexing according to the encryption/decryption security context identifier into the bank of initial variables to retrieve an initial variable for the source datablock, generating an output datablock from the source datablock and its corresponding initial variable, and replacing the initial variable

in the bank of initial variables with a new seed as determined by a selected mode of operation, for security context identifier.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

September 7, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

9/13/07